REMARKS

Applicant appreciates the thorough review of the present application as reflected in the Office Action. Claims 1-31 are pending and stand rejected under 35 U.S.C. §102(e) as anticipated by U.S. Patent Application Publication 2003/0110392 to Aucsmith et al. ("Aucsmith"). Claims 1, 15, and 26 have been amended.

Applicant has carefully examined Aucsmith and submits that Claims 1-31 are not anticipated for at least the following reasons. Accordingly, Applicant requests reconsideration and allowance of Claims 1-31.

Amended Drawings Overcome the Objections:

Figure 5 has been amended in the replacement sheets to correct the label between elements 520 and 530 to recite "Yes". Applicant therefore requests withdrawal of the objection to Figure 5.

Independent Claims 1, 15, and 26 are Not Anticipated by Aucsmith:

Independent Claim 1 recite that the method of responding to an intrusion includes selectively *responding to at least one notification of an intrusion*, from a network-accessible intrusion detection service (IDS) manager, by a computer evaluating the notification *based on local IDS policy that includes* information relating to the notification of an intrusion *and information related to the computer*. Claim 1 has been amended to further clarify that the computer hosts application programs accessible to users and, therefore, may be a personal computer. Support for this amendment is provided, for example, in the present application on page 7, lines 15-27.

The present application describes a possible advantage of having a host computer respond to an intrusion notice based on *local policies that include information relating to that computer* as follows:

> Accordingly, the host computer 300 decides whether and/or how it will respond to an intrusion notice based on local policies that include information relating to the computer. *Thus, in a computer networking system 302 that has numerous host computers 300, each host computer 300 may respond differently to an intrusion notice based on local information that is know to*

> *that host computer 300. In this way, how host computers 300 respond to intrusions can be individually customized. Such local customization of responses may enable improved automation of how host computers 300 respond to intrusions.*
> (Present Application, page 7, lines 7-14, emphasis added).

The Office Action suggests that the following paragraph 0055 of Aucsmith discloses the recitations of Claim 1 (emphasis added):

> [0055] *The server 104* may report the anomaly to the appropriate element or elements included in the network configuration 100 in real time and *subsequently determine if the anomaly constitutes an actual security problem*. In that case, the server 104 may needlessly report an anomaly if the anomaly turns out to not constitute an actual security problem. If, however, the implications of the anomaly are sufficiently severe, then reporting the anomaly as soon as possible may enable the client terminals 102(1)-102(N) to more quickly receive notice of the anomaly and may more quickly reduce or eliminate any harmful effects of the anomaly. *Waiting for the server 104 to complete a more detailed evaluation of the anomaly than the agent 106 already made before sending a report of the anomaly may incur a delay long enough for the client terminals 102(1)-102(N) to accept or pass information that would be identified as an anomaly using information in the report.*

Accordingly, paragraph 0055 of Aucsmith describes that the agent 106 within a client terminal 102 notifies the server 104 when an anomaly is detected, and that the server 104 then carries out analysis to determine if the anomaly constitutes an actual security problem. In paragraphs 0041-0043 Aucsmith describes that "if the agent 106 does detect a known anomaly, then the agent 160 reports 210 the anomaly to the server 104", that "once the agent 106 reports the anomaly, the agent 106 returns 200 to waiting for another piece of information to arrive at the client 102 or to examining a piece of information that previously arrived at the client 102, and that "the server 104 receives notice of the anomaly and can examine the anomaly to determine 214 if the anomaly constitutes an actual anomaly, e.g., a known security problem ... serious enough report to the client terminals 102(1)-102(N)." Thus, the agent 106 reports an anomaly to the server 104, and the server 104 determines whether the reported anomaly is a known security problem.

Aucsmith appears to stop-short of explaining what, if any, action the agent 106 would take in response to the server 104 determining that the reported anomaly is a known security problem. Indeed, nowhere does Aucsmith describe or suggest that the agent 106 would selectively respond to a security decision notification from the server 104 using information that is related to the agent 106, as opposed to responding to the notification without regard to information related to the agent 106. Accordingly, if the agents 106(1)-160(N-1) in client terminals 102(1)-102(N-1) were to receive such a security decision notification from the server 104, nothing in Aucsmith would appear to describe or suggest why or how any of the agents 106(1)-160(N-1) would respond differently from one another.

Accordingly, Applicant submits that neither paragraph 0055 nor elsewhere does Aucsmith describe or suggest a method of responding to an intrusion that includes selectively *responding to at least one notification of an intrusion*, from a network-accessible intrusion detection service (IDS) manager, by a computer evaluating the notification *based on local IDS policy that includes* information relating to the notification of an intrusion *and information related to the computer*. Consequently, Applicant submits that Aucsmith does not anticipate Claim 1 and, therefore, requests reconsideration and allowance of Claim 1.

Amended independent Claims 15 and 26 contains similar recitations to independent Claim 1, and are therefore submitted to not be anticipated by Aucsmith for at least the reasons explained above for Claim 1. Accordingly, reconsideration and allowance of Claims 15 and 26 is requested.

Dependent Claims 2-14, 16-25, and 27-31 are Not Anticipated by Aucsmith:

Dependent Claim 2 recites that the computer responds to the intrusion notification by evaluating the notification based on a local IDS policy and based on whether the computer, which hosts application programs accessible to users, is a firewall for other computers in the computer system. In rejecting Claim 2, the Office Action on page 4 cites element 112 in Figure 1 of Aucsmith, which is a firewall. However, the firewall 112 is not described in Aucsmith as a computer that hosts

application programs accessible to users. Moreover, Aucsmith does not appear to describe or suggest that the firewall 112 is configured to respond to intrusion notification based on a local IDS policy. Aucsmith describes the client terminal 102 as a computer that hosts application programs accessible to users, and hosts the agent 106. However, nowhere does Aucsmith describe or suggest that the client terminal 102/agent 106 evaluates an intrusion notification *based on a local IDS policy* and based on *whether the agent 106 is a firewall for other computers*. Consequently, Applicant submits that Claim 2 is not anticipated by Aucsmith.

Dependent Claims 3, 21, and 29 recite that the computer responds to the intrusion notification by evaluating the notification based on a local IDS policy and based on *whether the computer is a server of information for other computers in the computer system*. In rejecting Claims 3, 21, and 29, the Office Action on page 4 cites paragraphs 0030, 0033, and 0051-0055. However, neither the cited paragraphs nor elsewhere does Aucsmith describe or suggest that the agent 106 responds to an intrusion notification based on a local IDS policy and based on whether the agent 106 is a server of information for other computers. If the Office Action is reading these claims on the server 104, then Applicant notes that Aucsmith describes the server 104 as the IDS manager, Aucsmith does not describe or suggest that the server 104 is configured to respond to an intrusion notification from some other network accessible IDS manager and based on a local IDS policy. Consequently, Applicant submits that Claims 3, 21, and 29 are not anticipated by Aucsmith.

Dependent Claims 5, 22, and 30 recite that the computer responds to the intrusion notification by evaluating the notification based on a local IDS policy and based on *whether the computer is protected by a firewall* from a source of the intrusion. In rejection Claims 5, 22, and 30, the Office Action on page 5 again cites paragraphs cites paragraphs 0030, 0033, and 0051-0055 which briefly describes the firewall 112. As explained above, Aucsmith's description of the firewall 112 does not describe or suggest the recitations of these claims. Moreover, Applicant submits that neither the cited paragraphs nor elsewhere does Aucsmith describe or suggest that the agent 106 evaluates an intrusion notification *based on a local IDS policy* and based on

whether the agent 106 is a firewall for other computers. Consequently, Applicant submits that Claims 5, 22, and 30 are not anticipated by Aucsmith.

Dependent Claim 6 recites that the that the computer responds to the intrusion notification by evaluating the notification based on a *local IDS policy and based on memory utilization in the computer*. In rejecting Claim 6, the Office Action on page 5 cites paragraph 0084 of Aucsmith which is repeated below:

> [0084] The techniques described here are not limited to any particular hardware or software configuration; they may find applicability in any computing or processing environment. The techniques may be implemented in hardware, software, or a combination of the two. The techniques may be implemented in programs executing on programmable machines such as mobile or stationary computers, personal digital assistants, and similar devices that each include a processor, a storage medium readable by the processor (including volatile and non-volatile memory and/or storage elements), at least one input device, and one or more output devices. Program code is applied to data entered using the input device to perform the functions described and to generate output information. The output information is applied to one or more output devices.

Although Aucsmith mentions that its techniques may be carried out in computer memory, Applicant submits that nowhere does Aucsmith describe or suggest that the agent 106, or a host computer, responds to the intrusion notification by evaluating the notification based on a *local IDS policy and based on memory utilization in the computer*. Consequently, Applicant submits that Claim 6 is not anticipated by Aucsmith.

Dependent Claim 7 recites that the that the computer responds to the intrusion notification by evaluating the notification based on a *local IDS policy and based on processor utilization in the computer*. In rejecting Claim 7, the Office Action on page 5 again cites paragraph 0084 of Aucsmith. However, as described above, Aucsmith's paragraph 0084 does not describe or suggest that the agent 106, or a host computer, responds to the intrusion notification by evaluating the notification based on a *local IDS policy and based on processor utilization in the computer*. Consequently, Applicant submits that Claim 7 is not anticipated by Aucsmith.

Dependent Claims 9 and 25 recites that the that the computer responds to the intrusion notification by evaluating the notification based on a *local IDS policy and based on proximity of the computer to a source of the intrusion.* In rejecting these claims, the Office Action cites to paragraphs 0028 and 0051-0055. Applicants submit that neither the cited paragraphs nor elsewhere does Aucsmith describe that the agent 106, or any host computer, determines proximity of itself to a source of the intrusion or, much less, that it responds to an intrusion notification by evaluating a notification based on a *local IDS policy and based on proximity of the computer to a source of the intrusion.* Consequently, Applicant submits that Claims 9 and 25 are not anticipated by Aucsmith.

Dependent Claims 11 and 28 recite that a local IDS policy includes one or more response actions to be taken based on notification from the network-accessible IDS manager of an intrusion. As explained above, Aucsmith describes that the agent 106 identifies an anomaly and that the server 104 analyzes and confirms the anomaly. However, Aucsmith does not appear to describe or suggest what, if any, action the server 106 would take in response to an intrusion notification from the server 104. Moreover, applicant submits that Aucsmith does not describe or suggest that the agent 106 includes a local IDS policy that includes one or more response actions to be taken based on notification from the server 104. Consequently, Applicant submits that Claims 11 and 28 are not anticipated by Aucsmith.

Dependent Claims 12-14 further define that the response action includes terminating an application that is the target of an attack, discarding information in a communication to the computer, and discontinuing communication with a source of the communication, respectively. In rejecting these claims, the Office Action cites paragraphs 0037 and 0039 of Aucsmith. Applicant submits that neither the cited paragraphs nor elsewhere does Aucsmith describe or suggest what, if any action, the agent 106 would take in response to an intrusion notification from the server 104 and, much less, does not describe or suggest the specific actions recited in Claims 12-14. Consequently, Applicant submits that Claims 12-14 are not anticipated by Aucsmith.

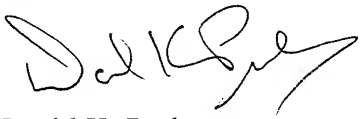
Dependent Claim 17 recites that at least two of the computers respond differently to the same intrusion notification from the IDS manager. The Office Action on page 7 cites paragraph 0055 to reject Claim 17. Applicant submits that neither paragraph 0055 nor elsewhere does Aucsmith describe or suggest that any of the agents 106(1)-106(N-1) would respond differently from one another to an intrusion notification from the server 104. Indeed, as explained above, Aucsmith does not describe or suggest that the agents 106(1)-106(N-1) would respond to a notice from the server 104 using an IDS policy and information related to that particular one of the agents and, consequently, does not appear to provide any operation by which one of the agents can respond differently than another one of the agents. Consequently, Applicant submits that Claim 17 is not anticipated by Aucsmith.

Claim 18 is similar to Claim 17 and is submitted to not be anticipated by Aucsmith for at least the reasons explained for Claim 17.

CONCLUSION

In light of the above amendments and remarks, Applicant respectfully submits that the above-entitled application is now in condition for allowance. Favorable reconsideration of this application is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

Respectfully submitted,



David K. Purks
Registration No. 40,133
Attorney for Applicant(s)

USPTO Customer No. 46589
Myers Bigel Sibley & Sajovec, P.A.
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401